Cyber Security Risk Assessment & Mitigation Plan

June 1, 2007

1.0 INTRODUCTION

The Office of Science (SC) Threat Statement (June 6, 2007) identifies multiple threats that are considered probable or possible[1]. These threats represent opportunities for multiple actors (individuals who orchestrate the attack) to exploit vulnerabilities in the DOE/SC infrastructure to either acquire or destroy information. SC realizes that while no information system can be totally protected there are specific risk mitigation controls and techniques that can be implemented to remediate many of the attack vectors. This document outlines the vulnerabilities that are unique to SC because of its mission to conduct basic research in a world-wide collaborative environment and the specific mitigation strategies and plans that are being implemented across the sub-element to reduce this exposure.

This document does not follow the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Risk Assessment*, methodology because the threats are considered credible and specific remediations are currently being implemented or are being rolled out. Therefore this document addresses vulnerabilities and documents the current efforts underway and future plans to minimize the risk to an acceptable level. Finally, this document will only address the specific actions that are being taken to reduce cyber risks. Natural and environmental threats are addressed in the safeguards and security risk mitigation plan.

1.1 PURPOSE

This document identifies the threats, foreign and domestic, to the SC Laboratories and Site Offices' information and information systems, and the specific risk management strategies, or controls being implemented to reduce the risks to an acceptable level. The following definitions apply:

- Threat: Any individual, organization, or activity that potentially could damage the confidentiality, integrity, or availability of information or information systems.
- Vulnerability: Any flaw or weakness in people, processes, technology, system security procedures, design, implementation or internal controls that could be exploited and result in a security breach or violation of the system's security policy.
- Risk: The net impact on mission, considering the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system's susceptibilities and the resulting impact if this should occur.
- Risk Management: The total process of identifying, controlling, and mitigating information system–related risks. This includes risk assessment; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.

1.2 BACKGROUND

SC has been assisting the SC Site Offices and Laboratories in the upgrade of their unclassified information systems security programs to comply with the latest requirements from the Office of

[1] Probable = greater than 75%, possible = between 50-75%

Management and Budget (OMB), NIST, and DOE. Since many of the Laboratories connect to networks they do not manage, allow unauthenticated remote access to scientists to run experiments, and develop software applications and documentation on assets that are housed on their premises, they face comparable risk situations that must be addressed. Part of the assistance is the transference of technical and operational "best practices" that cost effectively reduce risk. This document represents the cost effective strategies and controls the Laboratories and sub-elements have agreed to incorporate to assure that risks to unclassified information is maintained at acceptable levels.

2.0 HUMAN THREATS

Nation States and "trusted" individuals have been identified as the actors most likely to cause harm to the SC infrastructure. In an open research environment the traditional network infrastructure characterized as "hard on the outside but soft on the inside" needed to be significantly enhanced to minimize the risk of having information compromised as a result of the collaborative business mission.

SC has made tremendous strides in hardening the inside – this includes isolation of the open research network from the other information systems on the campus, assuring that only authorized users have access to the public network used for visitors, increased logging of user activities, and incorporating standardized secure configuration settings for the devices used to process, store and transmit information.

It is recognized that all risks cannot be mitigated by implementation of technical controls. Social engineering is still one of the most successful attack vectors and the "disgruntled or arrogant employee" is also a concern with respect to information compromise. Training and awareness have been improved over the last year to mitigate the social engineering vulnerability and many sites have incorporated tools to monitor "suspicious" behavior. Following are the identified threat sources and vulnerabilities that are unique to SC and the risk mitigation techniques or plans that are being consistently applied to reduce these to an acceptable level.

3.0 MITIGATION OF HUMAN THREATS UNIQUE TO SCIENCE

3.1 GENERAL RISK MITIGATION TECHNIQUES

In January 2002, the Carnegie Mellon University Software Engineering Institute's CERT Program (CERT) and the United States Secret Service (USSS) National Threat Assessment Center (NTAC) started a joint project, the Insider Threat Study.[2] The study combined NTAC's expertise in behavioral psychology with CERT's technical security expertise to provide in-depth analysis of approximately 150 insider incidents that occurred in critical infrastructure sectors between 1996 and 2002. Analysis included perusal of case documentation and interviews of personnel involved in the incident.

[2] The Insider Threat Study was funded by the USSS, as well as the Department of Homeland Security, Office of Science and Technology, which provided financial support for the study in fiscal years 2003 and 2004.

The results of the Insider Threat Study show that to detect insider threats as early as possible or to prevent them altogether management, IT, human resources, security officers, and others in the organization must understand the psychological, organizational, and technical aspects of the problem, as well as how they coordinate their actions over time.[3]

SC realizes that a strong cyber security program is predicated on people, process, and technology working together to address the vulnerabilities to information and information systems. The mitigation techniques include:

- Increased user awareness training
- Standardization of configuration setting on network devices
- Improved patch management
- Limitation on system administration rights
- Specialized user training
- Improvements in rigor of background checks
- Improved Intrusion Detection System (IDS) and Intrusion Protection System (IPS) systems
- Improved operational processes for log and audit reviews
- Improved cyber / HR coordination with employee transfers and terminations
- Two-factor authentication for information systems and networks holding sensitive (moderate or higher risk for confidentiality) information

It is expected that improvement in all these areas will reduce insider threat and the inherent vulnerability of having numerous long and short visitors (scientists) to the facilities with access to multiple information systems.

3.1.1 Nation States – Foreign Intelligence Services

Foreign Intelligence Services (FIS) represent the most sophisticated actor. Foreign nation-states have the tools and the personnel to conduct sustained attacks. The risks are two fold, as the attack could be centered on the compromise of one of the main nodes of the SC network to disrupt research or acquire information, or to seek use of the grid as a means to bridge to more private networks external to or within SC.

Risk mitigation actions and plans include the use of "honeypots[4]" within the business enclaves at some sites to entice an intruder to that server so the actions may be monitored and contained; development of custom software which can detect slow scans; use of commercial intrusion detection and intrusion prevention (IDS and IPS) software; specialized training for security monitoring staff on the latest attack strategies, vectors and tools; and isolation of the "open

[3] Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System Sabotage, D. Cappelli, etal.

[4] An Internet-attached server that acts as a decoy, luring in potential hackers in order to study their activities and monitor how they are able to break into a system.

research" enclaves from the rest of the facilities network. In addition, all network devices are patched and protected with anti-virus, anti-spam, and configuration restriction software.

Residual Risk: It is still possible for a Nation State to compromise SC assets by planting a Trojan for which the signature has not been identified or which is able to hide (e.g., rootkits) from traditional virus checking applications. However, in order for these attacks to be successful the system must be able to transmit the information they collect, and with IDS/IPS and system logging and auditing enabled, it is possible to detect this activity in the early stages.

3.1.2 Foreign National Visitors – Short Term

Foreign nationals who visit the Laboratories for a short duration are required to follow DOE Order 142.1, *Classified Visits Involving Foreign Nationals,* and DOE Order 142.3, *Unclassified Visits and Assignment Program*. These Orders define a specific process to confirm the identity of the individual as well as establish requirements for the hosting facility to assure that the visit is conducted according to processes defined in a specific security plan. Visitors on short term unclassified assignments are permitted access only to the public network to use internet e-mail services, or to the specific research network for which their security plan allows access. The research network by design is segmented from the business enclaves and from systems that may contain personally identifiable information (PII) or sensitive information. Furthermore, the majority of the short term visits are for conferences during which the visitor is usually limited to the public access areas of the facilities.

Residual Risk: Social engineering attacks can occur even when the individual is on a short term visit. The short-term visit may segue to a longer term assignment that can be promoted by the person being "socially engineered." The visitor may be granted a private tour of the facility and may record the event with a camera phone or other recording device. This is considered an acceptable risk as there is no classified or confidential information in these areas, and all visitors are required to leave all recording devices outside if access into controlled space is granted. Finally, social engineering attacks are discussed in awareness and counterintelligence training and additional training is required for personnel traveling abroad.

3.1.3 Foreign National Visitors – Long Term

All foreign national access to SC computing systems will be determined by the type of system to which the foreign national is requesting access. SC has three major types of systems as indicated below. Access is granted consistent with programmatic need, subject to a risk assessment taking into account the special circumstances for foreign national access. Each Laboratory must maintain a list of systems that fall into Type 2 and 3 below to assure that access to these systems for visiting foreign nationals is provided in accordance with the site's security plan.

1. Scientific Research Systems

These systems are used for scientific research and in general have no security restrictions specific to foreign nationals. Moreover, remote access to these systems by scientists worldwide is important for scientific collaboration.

The following personnel screening controls are required for users that have access to this class of information system. For **local users**, **local administrators** and **system administrators**, a Human Resource (HR) background check[5] is required for access by all employees.[6]

2. Infrastructure Systems

These systems are used to manage the "business end" of the Laboratories. These systems include: payroll, travel, human resources, finance and contracts; and many of these systems contain PII. Because of the additional risks involved in this type of access, any individual granted access must be formally approved by a process that includes consideration of such factors as place of birth and citizenship; as well as level of experience, judgment, training, and user privilege requested. All individuals granted access after this process must be approved by the system owner and the Information Security Officer.

The following screening controls are recommended for users that have access to this class of information system. For **local users** and **local administrators** and **system administrators,** a HR background check is required. For **domain administrators** a National Agency Check with Inquiries (NACI) must be conducted.

3. Controlled Information Systems

Certain computer systems or information systems contain or process export controlled information, Unclassified Controlled Nuclear Information (UCNI) data, etc. Access to such systems can only be granted to foreign nationals in a manner consistent with the DOE policy on foreign visits and assignments.

The following screening controls are required for users who have access to this class of information system:

For **local users**, an HR background check should be conducted. If the user is given access to a controlled information system, a National Agency Check with Law and Credit (NACLC) and Moderate Background Investigation (MBI) is required if the individual has established residency.

For **local administrators**, at a minimum, a NACI should be conducted. [If the user is given access to controlled information, a NACLC and MBI are required if the individual has established residency.]

---

[5] It is expected that this information will be provided as part of the Passport, Visa and Immigration and Naturalization Service Information request.

[6] There are four types of users discussed in the approach including:

- Local user – no ability to change configuration setting of the user workstation.
- Local Administrator – has ability to change the configuration settings of the user workstation.
- System Administrator - has ability to change the configuration settings of multiple workstations within the LAN segment.
- Domain Administrator – has the ability to configure network routers and gateways.

For **system administrators**, prior to access approval, at a minimum, a background investigation (BI) and NACI should be conducted. If the user is given access to controlled information system, a NACLC and Extensive Background Investigation (EBI) are required.

Residual Risk: Because long term visitors are often treated like regular employees (given a desk, workstation, badge, access to the network, etc.), it is easy to forget that in fact the individual is only visiting. Social engineering attacks have a higher likelihood of occurring and/or being successful because the individual is on site longer, and has access to "insider space" and the network. The opportunity to conduct malicious activities is also greater because the individual has unescorted access privileges and can move about freely with easy access to the networks. This risk is considered acceptable because all sites have upgraded the infrastructure with more robust IDS and IPS tools which would track suspicious behavior, and all servers have logging enabled so any attempts to access unauthorized information would be captured for later analysis. There would still be an opportunity to insert rootkits; however, the compromise would be apparent when the rootkit starts transmitting information.

3.1.4 Arrogant User

Also in this category can be the disgruntled user who has the ability to do similar damage albeit for different reasons. SC has taken steps to reduce the risks posed by arrogant users by implementing restrictive configuration settings on most of the workstations, requiring two factor authentication for remote access to systems that contain sensitive data and PII, enforcing appropriate use and code of conduct policies, and by enabling logging and auditing on all information servers. In addition, each site has implemented role based access controls which limit access to information sources. Many sites have implemented controls that alert the administration desk when a workstation or laptop changes configuration settings (for the limited population who maintain administrative rights), and most sites have war drivers that monitor the presence of wireless access points.

Future plans call for encryption software or copy prevention software (e.g., Sanctuary) on all workstations of individuals who process PII or other sensitive data, as well as two factor authentication even if the access is local. Workstations that handle sensitive information are required to utilize disk/information encryption software which will limit information loss.

Residual Risk: While the Laboratories and Site Offices have incorporated new technical controls and upgraded processes to limit the risk of the arrogant user, an arrogant user with system administration privileges is still a concern. SC is considering requiring an FBI background check for people with system or domain privileges as an additional protection measure. Furthermore, individuals with privileges are required to have specialized training which include awareness of their responsibilities and the requisite penalties for code of conduct violations.

3.1.5 Remote User – CONUS

Remote users that have a need to access resources in the Science research enclaves are given software to allow them to securely connect through a controlled gateway. Domestic users that need to access resources that contain sensitive information or PII are given secure ID tokens to confirm their identity when logging onto the network. Sites have improved the lag time between

when a contract ends and access is removed by implementation of exit and contract termination processes with HR.

Users that connect to Science resources domestically have their remote systems scanned to confirm the patch level of the operating system and that virus protection software is installed. Systems that are not patched and do not have a virus protection application installed and operational are to be denied access.

Users given passwords to access resources are required to sign a code of conduct agreement that prohibits the sharing of passwords. Violation of this agreement can result in suspension of access privileges. Students that have summer accounts are automatically "timed out" at the end of the summer period – this time out feature is established when the initial access is established.

3.1.6 Remote User – OCONUS

Remote access is not an exception in the open science world, it is the way SC operates. As such, SC has an approach through the NIST security framework that examines risk looking at the architecture, mission, operating environment, and cost to establish an appropriate level of security. That approach starts with a baseline set of controls and then incorporates numerous factors such as information sensitivity and the operating environment, tailors that set of baseline controls with compensating and supplementary controls to ensure that they are adequate based on risk. An important element in this approach is the separation of the research grid/enclaves from the rest of the SC internal network and servers. Access to the research grid simply provides a mechanism to access resources that by design are to be shared throughout the worldwide scientific community.

It is not possible to know who is on the grid - there is not an approved standard, nor is there an effective means to authenticate each user who may be on the grid. This is why logical separation is the primary access control being implemented within SC. In addition to logical separation constant patching of the routers, bridges, gateways, etc., are accomplished so that vulnerabilities to these devices are managed.

Residual Risk: The research itself is considered low risk as much of the information is shared, so the real concern is not acquisition of research information – but instead the possible destruction of it. Fortunately much of the scientific research consists of collections of petabytes of data and then distilling this information to analyze the megabytes of data that constitute the "useful" information. There is so much raw data that it would be extremely difficult to destroy it all. Also there are more experiments being run than there is time to analyze the information. Two of the Collider experiments have stored so much experimental data that analysis will be ongoing for five years after the Collider is decommissioned. Proprietary technologies and export controlled information are usually processed on workstations on an isolated subnet of the research enclave or in an enclave with moderate controls and only the scientists working on the program have access to these resources.

3.2 MITIGATION OF SPECIFIC VULNERABILITIES

There are a number of management and operational processes and technical controls that have been implemented to address the specific vulnerabilities addressed in the threat statement. The

list below reflects the remediation strategies that are planned or currently implemented to reduce these vulnerabilities to an acceptable level.

3.2.1 Failure to Patch Workstations and Laptops

The Site Visit technical assessment indicated that 9 of the 15 SC facilities did a credible job of patch management while the other 6 needed to improve this process. After the site visit process all sites were brought up to current patch levels for the operating systems being used for all the devices in the business enclaves. Systems that needed to remain below current patch level due to ongoing scientific experiments were isolated from the rest of the research network. When the experiments are concluded and the systems brought up to current patch level they are permitted to rejoin the main subnet of the research enclaves. The technical control of firewall isolation is being universally applied in all the SC Laboratories.

Another initiative underway is the replacement of older legacy systems that are no longer supported with newer systems that are part of the vendor patch management program. Legacy systems that cannot be replaced are firewalled from the rest of the environment. As with experimental systems that do not have the latest patches applied, legacy systems are also firewalled from the main campus network for the life of the legacy system.

Each SC site has plans to or has incorporated an asset management tool that constantly scans the network looking at the patch levels of the devices. Owners of devices that do not support the current level are notified of their deficiency and then electronically removed from the network if the requisite patches are not installed within a set period (usually 24 hours for critical patches). Devices that are not at the current patch level are not permitted to attach to the network.

3.2.2 Voice Over IP (VOIP) and Peer-to-Peer (P2P) Networking

VOIP vulnerabilities can be remediated by assuring that devices that support this protocol are up to date with required patches (see 3.1.1). Another concern is the possibility that the VOIP connection can be initiated without the users being aware. Network devices within the SC are configured to security restrictive settings which prohibit the remote initiation of VOIP services by disabling the remote listening feature. All sites are now required to subscribe to the weekly Microsoft Tuesday patch upload service to keep their system current with the patches that remediate high vulnerabilities in the operating system. Similar services are available from other vendors as exploits of feature rich services are a continual problem.

P2P networking is essential for sharing large amounts of information. The concern is that some servers may be used for sharing of copyrighted material or for illegal or illicit material. Risk mediation strategies include scans of the information servers for the most common files extension (wmv, mov, jpeg, MP3, wav, etc.) as well as to assure that these servers are not used for SPAM. Logging of activities and audits of the log records are operational controls that are use to assure that only scientific information is being shared. Finally, all workstations are configured such that information cannot be automatically uploaded via P2P – this control seeks to reduce the possibility that a machine configured to support P2P networking could have a Trojan inserted without user action.

3.2.3 Grid Computing

As stated above, because grid networks are composed of loosely coupled, heterogeneous resources managed by different administrators, they are far more vulnerable than single

administrator networks. Grid devices that are housed on domestic SC facilities are maintained (patched, configured, etc.) using the NIST SP 800-53 controls as part of a robust cyber security program; however, SC does not control/administer all the network nodes. Therefore, the grid infrastructure is completely isolated from the campus networks that are used for internal support services or for citizen centric servers. Furthermore, access to the grid is under physical security control, so one would have to bypass the physical security locks, personnel, and access control systems before any cyber access could be attained.

The ability to commandeer the grid to attack another government or commercial sector is possible, but any Nation State that initiates the attack would be identified quickly due to the forensic analysis capability of the counter-intelligence staff as well as the FBI and other agencies that would become involved. Thus the political and economic fallout from such an activity serves to keep this risk in check.

3.2.4 Mobile Devices – Laptops/PDA/Cell Phone

Laptops/PDA/Cell phones all are essential tools for the mobile individual; however precautions need to be taken to avoid compromise of information. The following management operational and technical controls have been incorporated throughout SC as appropriate use for these devices

1. Operational Control: Laptops are required to have a DOE approved password for access. PDA and Cell phones are required to have a PIN to access the keyboard or dial pad. When on foreign travel all mobile devices are to be within physical reach at all times until the destination is reached. When on foreign travel all information is to be carried on portable media (e.g., thumb-drive) and carried on the person. Users are encouraged to take a government issued travel laptop for foreign travel whenever possible.
2. Management Controls: User training includes awareness of proper phone etiquette with respect to conversations that can be overheard on the phone. Users are made aware that all phone conversations are easily intercepted and to refrain from discussing work related issues. When in public places, text messages are preferable to voice calls. Laptops may be used in public places and privacy screens are encouraged. Sensitive information may not be accessed in public places.
3. Technical Controls: Laptops are to have encryption software installed to protect sensitive information. The individual is at liberty to either protect just the sensitive information or encrypt the entire drive. Government issued PDAs have a safety kill feature which will permanently erase information if 10 incorrect PIN numbers are entered sequentially. All laptops are required to have anti-virus and other protective software to detect installation of malware.

3.2.5 Loss of PII

SC has multiple controls for the protection of PII. Access to information systems that contain PII are limited to individuals with a “need to know” and are placed in an enclave protected by NIST moderate controls. Individuals requiring access are usually in the Human Resources, Finance or Contracts departments. These individuals have only local user rights on their workstation, so there are restrictions on downloading PII to the workstation. Some managers and

department heads may have limited access to PII, but they use a dedicated machine and connection to access these systems. Transmission of PII requires Federal Information Processing Standards 140-2, Level 1 or higher encryption. There is also a recommendation to have all access to PII be via diskless workstations.

DOE and SC policy requires that all laptops have encryption software installed for the protection of PII and other sensitive information, in addition all portable media used to store PII must do so in encrypted format.

PII training for IT personnel was provided at a SC Cyber Security Working Group Workshop in July 2006. Two categories of PII were identified– that which is available in the public domain (name, phone number, address, etc) and that which requires protection controls (unique identification, numbers, health records, financial records, college transcripts, etc). Annual user awareness training has a specific module on the transmission, receipt, handling, storage and destruction of PII and sensitive information.

3.2.6 Extensive Use of System Administrator Rights

SC has been actively promoting (through the Site Visit program) policies and procedures that limit the number of personnel with administration rights. This program has been successful in greatly reducing the number of individuals with system administration privileges to people who actually perform system administration duties. Currently all users who access information system under moderate controls only have local user rights to their workstation. Many scientists who use government/contractor provided workstations and do not need to administer these workstations have had their system administration privileges removed. The goal of the effort is to reduce the number of personnel with system administration privileges to only those individuals who need it to perform work.

All facilities have or have plans to implement software that checks the configuration of the networked devices and will alert the support desk in the event that elevation of user rights is detected. Furthermore, all users that retain system administration privileges are trained to perform work on the most restricted access profile to accomplish the work.

3.2.7 Legacy Systems

SC has numerous legacy systems that host custom applications written by individuals who are no longer employed at the site. Often these custom applications have little or no documentation so rewriting the application for a newer operating system is very difficult. SC has implemented a two fold approach to legacy applications and servers. The first approach is a technical solution consisting of a dedicated firewall between all legacy systems and the wired infrastructure. This prevents a compromised legacy system from being used to elevate privileges on other resources on the network. As an additional control, the configuration settings of the device (if possible) are set to support the minimum number of services required for operation.

Another risk reduction control is a requirement that all developed software be consistent with Software Development Maturity Standard Level 3. This standard requires that all software be documented, and that user guides, administration guides and troubleshooting manuals be developed. While this control will not reduce the existing legacy applications, it will prevent additional undocumented applications from being developed.

3.2.8 Rootkits

The big problem with rootkits is they usually attach themselves to the boot firmware of a system, so these applications are not detected by traditional anti-virus/anti-spam software products. Using the stealth cloak provided by rootkits, spyware can operate undetected. An attacker can remotely install or modify components, steal locally stored personal information and even use the compromised machine for illegal activities.

To address the rootkits it is necessary to defend on all fronts. This includes:

- Prevention
- Detection
- Removal
- Monitoring

Kernel rootkit detection is extremely difficult because there is no separate process that can be terminated. In extreme cases, it can remove all traces of itself from the disk and completely hide inside the kernel. BIOS and virtual machine based rootkits are so difficult to remove that even rebuilding the system will not remove them.[7]

SC has implemented the only effective risk mitigation strategy which is education of the staff to avoid rootkit infection. This education includes awareness not to:

- download freeware which may contain rootkits
- open e-mail from unknown contacts
- download white papers, PowerPoint slides from un-sponsored or supported sites

Also the awareness training advises users to:

- report increased system latency times
- be suspicious if new applications require that special utilities are needed
- keep current with software patches – which help reduce user rootkit vulnerabilities

3.2.9 Social Engineering

There are multiple social engineering attack vectors, including phishing, telephone solicitation, delivery of advertisement media, and social contact. The only effective solution to avoid or mitigate social engineering attacks is training. The Office of Health, Safety and Security has conducted several social engineering exercises to determine susceptibility to social attacks. These exercises included emailed Trojans, spoofed URLs, phishing attacks, compromised CDs, Trojan thumb drives, and other methods to determine awareness. Lessons learned from these exercises have made all personnel aware of the myriad of social attacks.

The annual user awareness training and counter-intelligence training (for individuals on foreign travel) discuss social engineering attacks. The awareness training also reminds SC personnel that badges (permanent or visitor) are to be displayed and to "challenge" people who do not have

[7] Comment from rootkit briefing – DOE.

a badge. Awareness also reminds people that information can be compromised from shoulder surfing, dumpster diving and piggy backing into access controlled areas. Finally, the training reminds everyone to report suspicious behavior to the local security officer.

Glossary

Background Investigation (BI): Contact neighbors and former colleagues to confirm lifestyle, allegiance to country, loyalty; usually goes back 5 years

Domain Administrator: Has the ability to configure network routers and gateways

Extensive Background Investigation (EBI): Contact neighbors and former colleagues to confirm lifestyle, allegiance to country, loyalty; usually goes back 15 years.

Human Resource (HR) Background Check: Confirm employment dates, job functions, education.

Local Administrator: Privilege level that allows the user of the workstation or laptop to change configuration settings, download software, and create other users on the workstation or laptop.

Local User: Privilege level that restricts the user of the workstation or laptop from changing configuration settings, downloading software, and creating other users on the workstation or laptop.

Moderate Background Investigation (MBI): National Agency Check with Law and Credit (NACLC); contacts are made to neighbors.

National Agency Check (NAC): Part of every National Agency Check with Inquiries (NACI). Standard NACs are Security/Suitability Investigations Index (SII), Defense Clearance and Investigation Index (DCII), Federal Bureau of Investigations (FBI) Name Check, and FBI National Criminal History Fingerprint Check.

National Agency Check with Inquiries (NACI): The basic and minimum investigation required for all new Federal employees consist of a National Agency Check (NAC) with written inquiries and searches of records. These cover specific areas of an individual's background during the past 5 years (with inquiries sent to current and former employers, schools attended, references and local law authorities). Coverage includes:

- Employment – 5 years
- Education – 5 years and highest degree verified
- Residence – 3 years
- Law Enforcement – 5 years
- National Agency Check (NAC)

National Agency Check with Law and Credit (NACLC): Basic National Agency Checks (Security/Suitability Investigations Index, Defense Clearance and Investigations Index, fingerprint classification, and a search of the Federal Bureau of Investigation's investigative index). Credit search covering all residence, employment, and education locations during the last 7 years. Law Checks covering all locations of residence, employment, and education during the

last 5 years and to all locations of admitted arrest, confirms identity, credit history, legal history, reason for access.

System Administrator: has ability to change the configuration settings of multiple workstations within the LAN segment.